

Algebraic points on Shimura curves of $\Gamma_0(p)$ -type (II)

Keisuke Arai

Abstract

In the previous article, we classified the characters associated to algebraic points on Shimura curves of $\Gamma_0(p)$ -type, and over a quadratic field we showed that there are at most elliptic points on such a Shimura curve for every sufficiently large prime number p . In this article, we get a similar result for points over number fields of higher degree on Shimura curves of $\Gamma_0(p)$ -type.

Notation

For an integer $n \geq 1$ and a commutative group (or a commutative group scheme) G , let $G[n]$ denote the kernel of multiplication by n in G . For a field F , let $\text{char } F$ denote the characteristic of F , let \overline{F} denote an algebraic closure of F , let F^{sep} (resp. F^{ab}) denote the separable closure (resp. the maximal abelian extension) of F inside \overline{F} , and let $G_F = \text{Gal}(F^{\text{sep}}/F)$, $G_F^{\text{ab}} = \text{Gal}(F^{\text{ab}}/F)$. For a prime number p and a field F of characteristic 0, let $\theta_p : G_F \rightarrow \mathbb{F}_p^\times$ denote the mod p cyclotomic character. For a number field k , let h_k denote the class number of k ; fix an inclusion $k \hookrightarrow \mathbb{C}$ and take the algebraic closure \overline{k} inside \mathbb{C} ; let k_v denote the completion of k at v where v is a place (or a prime) of k ; let $k_{\mathbb{A}}$ denote the adèle ring of k ; and let $\mathbf{Ram}(k)$ denote the set of prime numbers which are ramified in k . For a number field or a local field k , let \mathcal{O}_k denote the ring of integers of k . For a scheme S and an abelian scheme A over S , let $\text{End}_S(A)$ denote the ring of endomorphisms of A defined over S . If $S = \text{Spec}(F)$ for a field F and if F'/F is a field extension, simply put $\text{End}_{F'}(A) := \text{End}_{\text{Spec}(F')}(A \times_{\text{Spec}(F)} \text{Spec}(F'))$ and $\text{End}(A) := \text{End}_{\overline{F}}(A)$. Let $\text{Aut}(A) := \text{Aut}_{\overline{F}}(A)$ be the group of automorphisms of A defined over \overline{F} . For a prime number p and an abelian variety A over a field F , let $T_p A := \varprojlim A[p^n](\overline{F})$ be the p -adic Tate module of A , where the inverse limit is taken with respect to multiplication by $p : A[p^{n+1}](\overline{F}) \rightarrow A[p^n](\overline{F})$.

1 Introduction

Let B be an indefinite quaternion division algebra over \mathbb{Q} . Let

$$d := \text{disc } B$$

be the discriminant of B . Then d is the product of an even number of distinct prime numbers, and $d > 1$. Fix a maximal order \mathcal{O} of B . For each prime number p not dividing d , fix an isomorphism

$$\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong M_2(\mathbb{Z}_p) \quad (1.1)$$

of \mathbb{Z}_p -algebras.

Definition 1.1. (cf. [4, p.591]) Let S be a scheme. A QM-abelian surface by \mathcal{O} over S is a pair (A, i) where A is an abelian surface over S (i.e. A is an abelian scheme over S of relative dimension 2), and $i : \mathcal{O} \hookrightarrow \text{End}_S(A)$ is an injective ring homomorphism (sending 1 to id). We consider that A has a left \mathcal{O} -action. We sometimes omit “by \mathcal{O} ” and simply write “a QM-abelian surface”.

Let M^B be the coarse moduli scheme over \mathbb{Q} parameterizing isomorphism classes of QM-abelian surfaces by \mathcal{O} . The notation M^B is permissible although we should write $M^{\mathcal{O}}$ instead of M^B ; for even if we replace \mathcal{O} by another maximal order \mathcal{O}' , we have a natural isomorphism $M^{\mathcal{O}} \cong M^{\mathcal{O}'}$ since \mathcal{O} and \mathcal{O}' are conjugate in B . Then M^B is a proper smooth curve over \mathbb{Q} , called a Shimura curve. For a prime number p not dividing d , let $M_0^B(p)$ be the coarse moduli scheme over \mathbb{Q} parameterizing isomorphism classes of triples (A, i, V) where (A, i) is a QM-abelian surface by \mathcal{O} and V is a left \mathcal{O} -submodule of $A[p]$ with \mathbb{F}_p -dimension 2. Then $M_0^B(p)$ is a proper smooth curve over \mathbb{Q} , which we call a Shimura curve of $\Gamma_0(p)$ -type. We have a natural map

$$\pi^B(p) : M_0^B(p) \longrightarrow M^B$$

over \mathbb{Q} defined by $(A, i, V) \longmapsto (A, i)$.

For real points on M^B , we know the following.

Theorem 1.2 ([9, Theorem 0, p.136]). *We have $M^B(\mathbb{R}) = \emptyset$.*

In the previous article, we showed that there are few points over quadratic fields on $M_0^B(p)$ for every sufficiently large prime number p , which is an analogue of the study of points on the modular curve $X_0(p)$ ([7], [8]; for related topics, see [2]).

Theorem 1.3 ([3, Theorem 1.3]). *Let k be a quadratic field which is not an imaginary quadratic field of class number one. Then there is a finite set $\mathcal{N}(k)$ of prime numbers depending on k which satisfies the following.*

(1) *If $B \otimes_{\mathbb{Q}} k \cong M_2(k)$, then $M_0^B(p)(k) = \emptyset$ holds for every prime number $p \notin \mathcal{N}(k)$ not dividing d .*

(2) *If $B \otimes_{\mathbb{Q}} k \not\cong M_2(k)$, then $M_0^B(p)(k) \subseteq \{\text{elliptic points of order 2 or 3}\}$ holds for every prime number $p \notin \mathcal{N}(k)$ not dividing d .*

We can identify $M_0^B(p)(\mathbb{C})$ with a quotient of the upper half-plane, and we use the notion of “elliptic points” in this context. We generalize Theorem 1.3 to points over number fields of higher degree on $M_0^B(p)$. The following is the main result of this article.

Theorem 1.4. *Let k be a finite Galois extension of \mathbb{Q} which does not contain the Hilbert class field of any imaginary quadratic field. Then there is a finite set $\mathcal{L}(k)$ of prime numbers depending on k which satisfies the following. Assume that there is a prime number q which splits completely in k and satisfies $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \not\cong M_2(\mathbb{Q}(\sqrt{-q}))$, and let $p > 4q$ be a prime number which also satisfies $p \geq 11$, $p \neq 13$, $p \nmid d$ and $p \notin \mathcal{L}(k)$.*

(1) *If $B \otimes_{\mathbb{Q}} k \cong M_2(k)$, then $M_0^B(p)(k) = \emptyset$.*

(2) *If $B \otimes_{\mathbb{Q}} k \not\cong M_2(k)$, then $M_0^B(p)(k) \subseteq \{\text{elliptic points of order 2 or 3}\}$.*

2 Galois representations associated to QM-abelian surfaces (generalities)

We consider the Galois representation associated to a QM-abelian surface. Take a prime number p not dividing d . Let F be a field with $\text{char } F \neq p$. Let (A, i) be a QM-abelian surface by \mathcal{O} over F . We have isomorphisms of \mathbb{Z}_p -modules:

$$\mathbb{Z}_p^4 \cong T_p A \cong \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong M_2(\mathbb{Z}_p).$$

The middle is also an isomorphism of left \mathcal{O} -modules; the last is also an isomorphism of \mathbb{Z}_p -algebras (which is fixed in (1.1)). We sometimes identify these \mathbb{Z}_p -modules. Take a \mathbb{Z}_p -basis

$$e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad e_3 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad e_4 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

of $M_2(\mathbb{Z}_p)$. Then the image of the natural map

$$M_2(\mathbb{Z}_p) \cong \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p \hookrightarrow \text{End}(T_p A) \cong M_4(\mathbb{Z}_p)$$

lies in $\left\{ \begin{pmatrix} X & 0 \\ 0 & X \end{pmatrix} \middle| X \in M_2(\mathbb{Z}_p) \right\}$. The action of the Galois group G_F on $T_p A$ induces a representation

$$\rho : G_F \longrightarrow \text{Aut}_{\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p}(T_p A) \subseteq \text{Aut}(T_p A) \cong \text{GL}_4(\mathbb{Z}_p),$$

where $\text{Aut}_{\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p}(T_p A)$ is the group of automorphisms of $T_p A$ commuting with the action of $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$. We often identify $\text{Aut}(T_p A) = \text{GL}_4(\mathbb{Z}_p)$. The above observation implies

$$\text{Aut}_{\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p}(T_p A) = \left\{ \begin{pmatrix} sI_2 & tI_2 \\ uI_2 & vI_2 \end{pmatrix} \middle| \begin{pmatrix} s & t \\ u & v \end{pmatrix} \in \text{GL}_2(\mathbb{Z}_p) \right\},$$

where $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Then the Galois representation ρ factors as

$$\rho : G_F \longrightarrow \left\{ \begin{pmatrix} sI_2 & tI_2 \\ uI_2 & vI_2 \end{pmatrix} \middle| \begin{pmatrix} s & t \\ u & v \end{pmatrix} \in \text{GL}_2(\mathbb{Z}_p) \right\} \subseteq \text{GL}_4(\mathbb{Z}_p).$$

Let

$$\bar{\rho} : G_F \longrightarrow \left\{ \begin{pmatrix} sI_2 & tI_2 \\ uI_2 & vI_2 \end{pmatrix} \mid \begin{pmatrix} s & t \\ u & v \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p) \right\} \subseteq \mathrm{GL}_4(\mathbb{F}_p)$$

be the reduction of ρ modulo p . Let

$$\bar{\rho}_{A,p} : G_F \longrightarrow \mathrm{GL}_2(\mathbb{F}_p) \quad (2.1)$$

denote the Galois representation induced from $\bar{\rho}$ by “ $\begin{pmatrix} s & t \\ u & v \end{pmatrix}$ ”, so that we have

$$\bar{\rho}_{A,p}(\sigma) = \begin{pmatrix} s & t \\ u & v \end{pmatrix} \text{ if } \bar{\rho}(\sigma) = \begin{pmatrix} sI_2 & tI_2 \\ uI_2 & vI_2 \end{pmatrix} \text{ for } \sigma \in G_F.$$

Suppose that $A[p](F^{\mathrm{sep}})$ has a left \mathcal{O} -submodule V with \mathbb{F}_p -dimension 2 which is stable under the action of G_F . We may assume $V = \mathbb{F}_p e_1 \oplus \mathbb{F}_p e_2 = \left\{ \begin{pmatrix} * & 0 \\ * & 0 \end{pmatrix} \right\}$. Since V is stable under the action of G_F , we find $\bar{\rho}_{A,p}(G_F) \subseteq \left\{ \begin{pmatrix} s & t \\ 0 & v \end{pmatrix} \right\} \subseteq \mathrm{GL}_2(\mathbb{F}_p)$. Let

$$\lambda : G_F \longrightarrow \mathbb{F}_p^\times \quad (2.2)$$

denote the character induced from $\bar{\rho}_{A,p}$ by “ s ”, so that $\bar{\rho}_{A,p}(\sigma) = \begin{pmatrix} \lambda(\sigma) & * \\ 0 & * \end{pmatrix}$ for $\sigma \in G_F$. Note that G_F acts on V by λ (i.e. $\bar{\rho}(\sigma)(v) = \lambda(\sigma)v$ for $\sigma \in G_F$, $v \in V$).

3 Automorphism groups

We consider the automorphism group of a QM-abelian surface. Let (A, i) be a QM-abelian surface by \mathcal{O} over a field F . Put

$$\mathrm{End}_{\mathcal{O}}(A) := \{f \in \mathrm{End}(A) \mid fi(g) = i(g)f \text{ for any } g \in \mathcal{O}\}$$

and

$$\mathrm{Aut}_{\mathcal{O}}(A) := \mathrm{Aut}(A) \cap \mathrm{End}_{\mathcal{O}}(A).$$

If $\mathrm{char} F = 0$, then $\mathrm{Aut}_{\mathcal{O}}(A) \cong \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/6\mathbb{Z}$.

Let p be a prime number not dividing d . Let (A, i, V) be a triple where (A, i) is a QM-abelian surface by \mathcal{O} over a field F and V is a left \mathcal{O} -submodule of $A[p](\bar{F})$ with \mathbb{F}_p -dimension 2. Define a subgroup $\mathrm{Aut}_{\mathcal{O}}(A, V)$ of $\mathrm{Aut}_{\mathcal{O}}(A)$ by

$$\mathrm{Aut}_{\mathcal{O}}(A, V) := \{f \in \mathrm{Aut}_{\mathcal{O}}(A) \mid f(V) = V\}.$$

Assume $\mathrm{char} F = 0$. Then $\mathrm{Aut}_{\mathcal{O}}(A, V) \cong \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/6\mathbb{Z}$. Notice that we have $\mathrm{Aut}_{\mathcal{O}}(A) \cong \mathbb{Z}/2\mathbb{Z}$ (resp. $\mathrm{Aut}_{\mathcal{O}}(A, V) \cong \mathbb{Z}/2\mathbb{Z}$) if and only if $\mathrm{Aut}_{\mathcal{O}}(A) = \{\pm 1\}$ (resp. $\mathrm{Aut}_{\mathcal{O}}(A, V) = \{\pm 1\}$).

4 Fields of definition

Let k be a number field. Let p be a prime number not dividing d . Take a point

$$x \in M_0^B(p)(k).$$

Let $x' \in M^B(k)$ be the image of x by the map $\pi^B(p) : M_0^B(p) \longrightarrow M^B$. Then x' is represented by a QM-abelian surface (say (A_x, i_x)) over \bar{k} , and x is represented by a triple (A_x, i_x, V_x) where V_x is a left \mathcal{O} -submodule of $A[p](\bar{k})$ with \mathbb{F}_p -dimension 2. For a finite extension M of k (in \bar{k}), we say that we can take (A_x, i_x) (resp. (A_x, i_x, V_x)) to be defined over M if there is a QM-abelian surface (A, i) over M such that $(A, i) \otimes_M \bar{k}$ is isomorphic to (A_x, i_x) (resp. if there is a QM-abelian surface (A, i) over M and a left \mathcal{O} -submodule V of $A[p](\bar{k})$ with \mathbb{F}_p -dimension 2 stable under the action of G_M such that there is an isomorphism between $(A, i) \otimes_M \bar{k}$ and (A_x, i_x) under which V corresponds to V_x). Put

$$\text{Aut}(x) := \text{Aut}_{\mathcal{O}}(A_x, V_x), \quad \text{Aut}(x') := \text{Aut}_{\mathcal{O}}(A_x).$$

Then $\text{Aut}(x)$ is a subgroup of $\text{Aut}(x')$. Note that x is an elliptic point of order 2 (resp. 3) if and only if $\text{Aut}(x) \cong \mathbb{Z}/4\mathbb{Z}$ (resp. $\text{Aut}(x) \cong \mathbb{Z}/6\mathbb{Z}$).

Since x is a k -rational point, we have ${}^\sigma x = x$ for any $\sigma \in G_k$. Then, for any $\sigma \in G_k$, there is an isomorphism

$$\phi_\sigma : {}^\sigma(A_x, i_x, V_x) \longrightarrow (A_x, i_x, V_x),$$

which we fix once for all. Let

$$\phi'_\sigma : {}^\sigma(A_x, i_x) \longrightarrow (A_x, i_x)$$

be the isomorphism induced from ϕ_σ by forgetting V_x . For $\sigma, \tau \in G_k$, put

$$c_x(\sigma, \tau) := \phi_\sigma \circ {}^\sigma \phi_\tau \circ \phi_{\sigma\tau}^{-1} \in \text{Aut}(x)$$

and

$$c'_x(\sigma, \tau) := \phi'_\sigma \circ {}^\sigma \phi'_\tau \circ (\phi'_{\sigma\tau})^{-1} \in \text{Aut}(x').$$

Then c_x (resp. c'_x) is a 2-cocycle and defines a cohomology class $[c_x] \in H^2(G_k, \text{Aut}(x))$ (resp. $[c'_x] \in H^2(G_k, \text{Aut}(x'))$). Here the action of G_k on $\text{Aut}(x)$ (resp. $\text{Aut}(x')$) is defined in a natural manner (cf. [3, Section 4]).

Proposition 4.1 ([5, Theorem (1.1), p.93]). *We can take (A_x, i_x) to be defined over k if and only if $B \otimes_{\mathbb{Q}} k \cong M_2(k)$.*

Proposition 4.2 ([3, Proposition 4.2]). *(1) Suppose $B \otimes_{\mathbb{Q}} k \cong M_2(k)$. Further assume $\text{Aut}(x) \neq \{\pm 1\}$ or $\text{Aut}(x') \not\cong \mathbb{Z}/4\mathbb{Z}$. Then we can take (A_x, i_x, V_x) to be defined over k .*

(2) Assume $\text{Aut}(x) = \{\pm 1\}$. Then there is a quadratic extension K of k such that we can take (A_x, i_x, V_x) to be defined over K .

Lemma 4.3 ([3, Lemma 4.3]). *Let K be a quadratic extension of k . Assume $\text{Aut}(x) = \{\pm 1\}$. Then the following two conditions are equivalent.*

- (1) We can take (A_x, i_x, V_x) to be defined over K .*
- (2) For any place v of k satisfying $[c_x]_v \neq 0$, the tensor product $K \otimes_k k_v$ is a field.*

5 Classification of characters (I)

We keep the notation in Section 4. Throughout this section, assume $\text{Aut}(x) = \{\pm 1\}$. Let K be a quadratic extension of k which satisfies the equivalent conditions in Lemma 4.3. Then x is represented by a triple (A, i, V) , where (A, i) is a QM-abelian surface over K and V is a left \mathcal{O} -submodule of $A[p](\overline{K})$ with \mathbb{F}_p -dimension 2 stable under the action of G_K . Let

$$\lambda : G_K \longrightarrow \mathbb{F}_p^\times$$

be the character associated to V in (2.2). For a prime \mathfrak{l} of k (resp. K), let $I_{\mathfrak{l}}$ denote the inertia subgroup of G_k (resp. G_K) at \mathfrak{l} .

Let $\lambda^{\text{ab}} : G_K^{\text{ab}} \longrightarrow \mathbb{F}_p^\times$ be the natural map induced from λ . Put

$$\varphi := \lambda^{\text{ab}} \circ \text{tr}_{K/k} : G_k \longrightarrow G_K^{\text{ab}} \longrightarrow \mathbb{F}_p^\times \quad (5.1)$$

where $\text{tr}_{K/k} : G_k \longrightarrow G_K^{\text{ab}}$ is the transfer map. Notice that the induced map $\text{tr}_{K/k}^{\text{ab}} : G_k^{\text{ab}} \longrightarrow G_K^{\text{ab}}$ from $\text{tr}_{K/k}$ corresponds to the natural inclusion $k_{\mathbb{A}}^\times \hookrightarrow K_{\mathbb{A}}^\times$ via class field theory ([10, Theorem 8 in §9 of Chapter XIII, p.276]). We know that φ^{12} is unramified at every prime of k not dividing p ([3, Corollary 5.2]), and so φ^{12} corresponds to a character of the ideal group $\mathfrak{I}_k(p)$ consisting of fractional ideals of k prime to p . By abuse of notation, let denote also by φ^{12} the corresponding character of $\mathfrak{I}_k(p)$.

Let \mathcal{M} be the set of prime numbers q such that q splits completely in k and q does not divide $6h_k$. Let \mathcal{N} be the set of primes \mathfrak{q} of k such that \mathfrak{q} divides some prime number $q \in \mathcal{M}$. Take a finite subset $\emptyset \neq \mathcal{S} \subseteq \mathcal{N}$ which generates the ideal class group of k . For each prime $\mathfrak{q} \in \mathcal{S}$, fix an element $\alpha_{\mathfrak{q}} \in \mathcal{O}_k \setminus \{0\}$ satisfying $\mathfrak{q}^{h_k} = \alpha_{\mathfrak{q}} \mathcal{O}_k$.

For a prime number q , put

$$\mathcal{FR}(q) := \{ \beta \in \mathbb{C} \mid \beta^2 + a\beta + q = 0 \text{ for some integer } a \in \mathbb{Z} \text{ with } |a| \leq 2\sqrt{q} \}.$$

Notice that $|a| \leq 2\sqrt{q}$ implies $|a| < 2\sqrt{q}$ since $2\sqrt{q}$ is not a rational number. For $\mathfrak{q} \in \mathcal{S}$, put $N(\mathfrak{q}) = \sharp(\mathcal{O}_k/\mathfrak{q})$. Then $N(\mathfrak{q})$ is a prime number. Define the sets $\mathcal{M}_1(k) :=$

$$\left\{ (\mathfrak{q}, \varepsilon_0, \beta_{\mathfrak{q}}) \mid \mathfrak{q} \in \mathcal{S}, \varepsilon_0 = \sum_{\sigma \in \text{Gal}(k/\mathbb{Q})} a_{\sigma} \sigma \text{ with } a_{\sigma} \in \{0, 8, 12, 16, 24\}, \beta_{\mathfrak{q}} \in \mathcal{FR}(N(\mathfrak{q})) \right\},$$

$$\mathcal{M}_2(k) := \{ \text{Norm}_{k(\beta_{\mathfrak{q}})/\mathbb{Q}}(\alpha_{\mathfrak{q}}^{\varepsilon_0} - \beta_{\mathfrak{q}}^{24h_k}) \in \mathbb{Z} \mid (\mathfrak{q}, \varepsilon_0, \beta_{\mathfrak{q}}) \in \mathcal{M}_1(k) \} \setminus \{0\},$$

$$\mathcal{N}_0(k) := \{ l : \text{prime number} \mid l \text{ divides some integer } m \in \mathcal{M}_2(k) \},$$

$$\mathcal{T}(k) := \{ l' : \text{prime number} \mid l' \text{ is divisible by some prime } \mathfrak{q}' \in \mathcal{S} \} \cup \{2, 3\},$$

$$\mathcal{N}_1(k) := \mathcal{N}_0(k) \cup \mathcal{T}(k) \cup \mathbf{Ram}(k).$$

Notice that all of $\mathcal{FR}(q), \mathcal{M}_1(k), \mathcal{M}_2(k), \mathcal{N}_0(k), \mathcal{T}(k), \mathcal{N}_1(k)$ are finite.

Theorem 5.1 ([3, Theorem 5.6]). *Assume that k is Galois over \mathbb{Q} . If $p \notin \mathcal{N}_1(k)$ (and if p does not divide d), then the character $\varphi : G_k \longrightarrow \mathbb{F}_p^\times$ is of one of the following types.*

Type 2: $\varphi^{12} = \theta_p^{12}$ and $p \equiv 3 \pmod{4}$.

Type 3: There is an imaginary quadratic field L satisfying the following two conditions.

- (a) The Hilbert class field H_L of L is contained in k .
- (b) There is a prime \mathfrak{p}_L of L lying over p such that $\varphi^{12}(\mathfrak{a}) \equiv \delta^{24} \pmod{\mathfrak{p}_L}$ holds for any fractional ideal \mathfrak{a} of k prime to p . Here δ is any element of L such that $\text{Norm}_{k/L}(\mathfrak{a}) = \delta \mathcal{O}_L$.

From now to the end of this section, assume that k is Galois over \mathbb{Q} .

Lemma 5.2 ([3, Lemma 5.11]). *Suppose $p \geq 11$, $p \neq 13$ and $p \notin \mathcal{N}_1(k)$. Further assume the following two conditions.*

- (a) Every prime \mathfrak{p} of k above p is inert in K/k .
- (b) Every prime $\mathfrak{q} \in \mathcal{S}$ is ramified in K/k .

If φ is of type 2, then we have the following.

- (i) The character $\lambda^{12}\theta_p^{-6} : G_K \rightarrow \mathbb{F}_p^\times$ is unramified everywhere.
- (ii) The map $Cl_K \rightarrow \mathbb{F}_p^\times$ induced from $\lambda^{12}\theta_p^{-6}$ is trivial on $C_{K/k} := \text{Im}(Cl_k \rightarrow Cl_K)$, where Cl_K is the ideal class group of K and $Cl_k \rightarrow Cl_K$ is the map defined by $[\mathfrak{a}] \mapsto [\mathfrak{a}\mathcal{O}_K]$.

Lemma 5.3 ([3, Lemma 5.12]). *Suppose $p \geq 11$, $p \neq 13$ and $p \notin \mathcal{N}_1(k)$. Assume that φ is of type 2. Let $q < \frac{p}{4}$ be a prime number which splits completely in k . Then we have $\left(\frac{q}{p}\right) = -1$ and $q^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.*

From now to the end of this section, assume that we are in the situation of Lemma 5.3. Take a prime \mathfrak{q} of k above q . By replacing K if necessary, we may assume the conditions (a), (b) in Lemma 5.2 and that \mathfrak{q} is ramified in K/k (cf. [3, Remark 4.4]). Let \mathfrak{q}_K be the unique prime of K above \mathfrak{q} . The abelian surface $A \otimes_K K_{\mathfrak{q}_K}$ has good reduction after a totally ramified finite extension $M/K_{\mathfrak{q}_K}$. Let \tilde{A} be the special fiber of the Néron model of $A \otimes_K M$. Then \tilde{A} is a QM-abelian surface by \mathcal{O} over the prime field \mathbb{F}_q . We have $\lambda(\text{Frob}_M) \equiv \beta$ modulo a prime \mathfrak{p}_0 of $\mathbb{Q}(\beta)$ above p for a Frobenius eigenvalue β of \tilde{A} , where Frob_M is the arithmetic Frobenius of $G_M (\subseteq G_{K_{\mathfrak{q}_K}})$. We know $\beta \in \mathcal{FR}(q)$ by [5, p.97]. We also have $\lambda^{-1}\theta_p(\text{Frob}_M) \equiv \bar{\beta} \pmod{\mathfrak{p}_0}$, where $\bar{\beta}$ is the complex conjugate of β . Put $\psi := \lambda\theta_p^{-\frac{p+1}{4}}$. Then $\psi^{12} = \lambda^{12}\theta_p^{-3(p+1)} = \lambda^{12}\theta_p^{-6}$. By Lemma 5.2 (ii), we have $1 = \lambda^{12}(\mathfrak{q}\mathcal{O}_K)\theta_p^{-6}(\mathfrak{q}\mathcal{O}_K) = \psi^{12}(\mathfrak{q}\mathcal{O}_K) = \psi^{24}(\mathfrak{q}_K) = \psi^{24}(\text{Frob}_M) = \psi(\text{Frob}_M)^{24}$. Here, note that $\psi(\text{Frob}_M)$ is well-defined and that the fourth equality holds because the extension $M/K_{\mathfrak{q}_K}$ is totally ramified. Since \mathbb{F}_p^\times is a cyclic group of order $p-1$ and $p-1 \equiv 2 \pmod{4}$, we have $\psi(\text{Frob}_M)^6 = 1$.

Lemma 5.4. $(\beta + \bar{\beta})^2 \equiv 3q$ or $0 \pmod{p}$.

Proof. We have $\beta^2 + \bar{\beta}^2 \equiv \psi(\text{Frob}_M)^2\theta_p(\text{Frob}_M)^{\frac{p+1}{2}} + \psi(\text{Frob}_M)^{-2}\theta_p(\text{Frob}_M)^{-\frac{p+3}{2}} = \theta_p(\text{Frob}_M)^{\frac{p+1}{2}}(\psi(\text{Frob}_M)^2 + \psi(\text{Frob}_M)^{-2}) = q^{\frac{p+1}{2}}(\psi(\text{Frob}_M)^2 + \psi(\text{Frob}_M)^{-2}) \pmod{p}$. Since $\psi(\text{Frob}_M)^6 = 1$, we see $\psi(\text{Frob}_M)^2 + \psi(\text{Frob}_M)^{-2} = -1$ or 2 . Since $q^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, we have $q^{\frac{p+1}{2}} \equiv -q \pmod{p}$. Then $\beta^2 + \bar{\beta}^2 \equiv q$ or $-2q \pmod{p}$, and so $(\beta + \bar{\beta})^2 \equiv 3q$ or $0 \pmod{p}$. □

Lemma 5.5. $\beta + \overline{\beta} = 0$ or $|\beta + \overline{\beta}| = 3 = q$.

Proof. We have $(\beta + \overline{\beta})^2 < 4q$ since $\beta \in \mathcal{FR}(q)$. First assume $(\beta + \overline{\beta})^2 \equiv 3q \pmod{p}$. Then, since $|(\beta + \overline{\beta})^2 - 3q| \leq 3q < p$, we have $(\beta + \overline{\beta})^2 = 3q$. Therefore $q = 3$ and $\beta + \overline{\beta} = \pm 3$. Next assume $(\beta + \overline{\beta})^2 \equiv 0 \pmod{p}$. Then, since $|(\beta + \overline{\beta})^2| < 4q < p$, we have $(\beta + \overline{\beta})^2 = 0$. Therefore $\beta + \overline{\beta} = 0$. \square

Lemma 5.6. $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \cong M_2(\mathbb{Q}(\sqrt{-q}))$.

Proof. The number β is a Frobenius eigenvalue of a QM-abelian surface \tilde{A} by \mathcal{O} over \mathbb{F}_q . Then, by Lemma 5.5 and [5, Theorem 2.1 (2) (4) and Proposition 2.3, p.98], we conclude $\text{End}_{\mathbb{F}_q}(\tilde{A}) \otimes_{\mathbb{Z}} \mathbb{Q} \cong M_2(\mathbb{Q}(\sqrt{-q})) \cong B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q})$. \square

6 Classification of characters (II)

Let k be a number field, and let (A, i) be a QM-abelian surface by \mathcal{O} over k . For a prime number p not dividing d , assume that the representation $\overline{\rho}_{A,p}$ in (2.1) is reducible. Then there is a 1-dimensional sub-representation of $\overline{\rho}_{A,p}$; let ν be its associated character. In this case notice that there is a left \mathcal{O} -submodule V of $A[p](\overline{k})$ with \mathbb{F}_p -dimension 2 on which G_k acts by ν , and so the triple (A, i, V) determines a point of $M_0^B(p)(k)$. We know that ν^{12} is unramified at every prime of k not dividing p ([3, Lemma 6.1]), and so ν^{12} corresponds to a character of $\mathfrak{I}_k(p)$. By abuse of notation, let denote also by ν^{12} the corresponding character of $\mathfrak{I}_k(p)$.

Define the finite sets $\mathcal{M}'_1(k) :=$

$$\left\{ (\mathfrak{q}, \varepsilon'_0, \beta_{\mathfrak{q}}) \mid \mathfrak{q} \in \mathcal{S}, \varepsilon'_0 = \sum_{\sigma \in \text{Gal}(k/\mathbb{Q})} a'_\sigma \sigma \text{ with } a'_\sigma \in \{0, 4, 6, 8, 12\}, \beta_{\mathfrak{q}} \in \mathcal{FR}(N(\mathfrak{q})) \right\},$$

$$\mathcal{M}'_2(k) := \left\{ \text{Norm}_{k(\beta_{\mathfrak{q}})/\mathbb{Q}}(\alpha_{\mathfrak{q}}^{\varepsilon'_0} - \beta_{\mathfrak{q}}^{12h_k}) \in \mathbb{Z} \mid (\mathfrak{q}, \varepsilon'_0, \beta_{\mathfrak{q}}) \in \mathcal{M}'_1(k) \right\} \setminus \{0\},$$

$$\mathcal{N}'_0(k) := \{ l : \text{prime number} \mid l \text{ divides some integer } m \in \mathcal{M}'_2(k) \},$$

$$\mathcal{N}'_1(k) := \mathcal{N}'_0(k) \cup \mathcal{T}(k) \cup \mathbf{Ram}(k).$$

We classify the character ν as follows.

Theorem 6.1 ([3, Theorem 6.4]). *Assume that k is Galois over \mathbb{Q} . If $p \notin \mathcal{N}'_1(k)$ (and if p does not divide d), then the character $\nu : G_k \longrightarrow \mathbb{F}_p^\times$ is of one of the following types.*

Type 2: $\nu^{12} = \theta_p^6$ and $p \equiv 3 \pmod{4}$.

Type 3: There is an imaginary quadratic field L satisfying the following two conditions.

(a) The Hilbert class field H_L of L is contained in k .

(b) There is a prime \mathfrak{p}_L of L lying over p such that $\nu^{12}(\mathfrak{a}) \equiv \delta^{12} \pmod{\mathfrak{p}_L}$ holds for any fractional ideal \mathfrak{a} of k prime to p . Here δ is any element of L such that $\text{Norm}_{k/L}(\mathfrak{a}) = \delta \mathcal{O}_L$.

From now to Lemma 6.3, assume that k is Galois over \mathbb{Q} .

Lemma 6.2 ([3, Lemma 6.6]). *Suppose $p \notin \mathcal{N}'_1(k)$. If ν is of type 2, then there is a character $\psi' : G_k \rightarrow \mathbb{F}_p^\times$ such that $\psi'^6 = 1$ and $\nu = \psi' \theta_p^{\frac{p+1}{4}}$.*

Lemma 6.3 ([3, Lemma 6.7]). *Suppose $p \notin \mathcal{N}'_1(k)$. Assume that ν is of type 2. Let $q < \frac{p}{4}$ be a prime number which splits completely in k . Then we have $\left(\frac{q}{p}\right) = -1$ and $q^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.*

We can show the following lemma in the same way (Lemma 5.4 – Lemma 5.6) as in the last section.

Lemma 6.4. *In the situation of Lemma 6.3, we have $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \cong M_2(\mathbb{Q}(\sqrt{-q}))$.*

Theorem 6.5. *Let k be a finite Galois extension of \mathbb{Q} which does not contain the Hilbert class field of any imaginary quadratic field. Assume that there is a prime number q which splits completely in k and satisfies $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \not\cong M_2(\mathbb{Q}(\sqrt{-q}))$. Let $p > 4q$ be a prime number which also satisfies $p \nmid d$ and $p \notin \mathcal{N}'_1(k)$. Then the representation*

$$\bar{\rho}_{A,p} : G_k \rightarrow \mathrm{GL}_2(\mathbb{F}_p)$$

is irreducible.

Proof. Assume that $\bar{\rho}_{A,p}$ is reducible. Then the associated character ν is of type 2 in Theorem 6.1, because k does not contain the Hilbert class field of any imaginary quadratic field. By Lemma 6.4, we have $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \cong M_2(\mathbb{Q}(\sqrt{-q}))$, which is a contradiction. □

(Proof of Theorem 1.4)

Let k be a finite Galois extension of \mathbb{Q} which does not contain the Hilbert class field of any imaginary quadratic field, and let q be a prime number which splits completely in k and satisfies $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \not\cong M_2(\mathbb{Q}(\sqrt{-q}))$. Let $p > 4q$ be a prime number which also satisfies $p \geq 11$, $p \neq 13$ and $p \nmid d$. Take a point $x \in M_0^B(p)(k)$.

(1) Suppose $B \otimes_{\mathbb{Q}} k \cong M_2(k)$.

(1-i) Assume $\mathrm{Aut}(x) \neq \{\pm 1\}$ or $\mathrm{Aut}(x') \not\cong \mathbb{Z}/4\mathbb{Z}$. Then x is represented by a triple (A, i, V) defined over k by Proposition 4.2 (1), and the representation $\bar{\rho}_{A,p}$ is reducible. By Theorem 6.5, we have $p \in \mathcal{N}'_1(k)$.

(1-ii) Assume otherwise (i.e. $\mathrm{Aut}(x) = \{\pm 1\}$ and $\mathrm{Aut}(x') \cong \mathbb{Z}/4\mathbb{Z}$). Then x is represented by a triple (A, i, V) defined over a quadratic extension of k by Proposition 4.2 (2), and we have a character $\varphi : G_k \rightarrow \mathbb{F}_p^\times$ as in (5.1). By Theorem 5.1 and Lemma 5.6, we have $p \in \mathcal{N}'_1(k)$.

(2) Suppose $B \otimes_{\mathbb{Q}} k \not\cong M_2(k)$. Further assume that x is not an elliptic point of order 2 or 3; this implies $\mathrm{Aut}(x) = \{\pm 1\}$. By the same argument as in (1-ii), we conclude $p \in \mathcal{N}'_1(k)$. □

7 Examples

The genus of the Shimura curve M^B is 0 if and only if $d \in \{6, 10, 22\}$ ([1, Lemma 3.1, p.168]). The defining equations of such M^B 's are the following by [6, Theorem 1-1, p.279].

$$\begin{cases} d = 6 : x^2 + y^2 + 3 = 0, \\ d = 10 : x^2 + y^2 + 2 = 0, \\ d = 22 : x^2 + y^2 + 11 = 0. \end{cases}$$

In these cases, for a field k of characteristic 0 the condition $M^B(k) \neq \emptyset$ implies $M^B \otimes_{\mathbb{Q}} k \cong \mathbb{P}_k^1$, and so $\#M^B(k) = \infty$.

In the following proposition, we give some examples of Theorem 1.4.

Proposition 7.1. *Let $d \in \{10, 22\}$ and $k \in \{\mathbb{Q}(\sqrt{-5}, \sqrt{7}), \mathbb{Q}(\zeta_{13})\}$. Then we have the following.*

- (1) *k does not contain the Hilbert class field of any imaginary quadratic field.*
- (2) *The least prime number q that splits completely in k and satisfies $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \not\cong M_2(\mathbb{Q}(\sqrt{-q}))$ is 29 (resp. 29, resp. 79, resp. 79) for $(d, K) = (10, \mathbb{Q}(\sqrt{-5}, \sqrt{7}))$ (resp. $(22, \mathbb{Q}(\sqrt{-5}, \sqrt{7}))$, resp. $(10, \mathbb{Q}(\zeta_{13}))$, resp. $(22, \mathbb{Q}(\zeta_{13}))$).*
- (3) *$\#M^B(k) = \infty$.*
- (4) *$B \otimes_{\mathbb{Q}} k \cong M_2(k)$.*
- (5) *$M_0^B(p)(k) = \emptyset$ for every sufficiently large prime number p .*

Remark 7.2. If $d = 6$ and $k \in \{\mathbb{Q}(\sqrt{-5}, \sqrt{7}), \mathbb{Q}(\zeta_{13})\}$, then $M^B(k) = \emptyset$. In this case $M_0^B(p)(k) = \emptyset$ for any prime number p (not dividing d).

References

- [1] *K. Arai*, On the Galois images associated to QM-abelian surfaces, Proceedings of the Symposium on Algebraic Number Theory and Related Topics, 165–187, RIMS Kôkyûroku Bessatsu, **B4**, Res. Inst. Math. Sci. (RIMS), Kyoto, 2007.
- [2] *K. Arai*, Galois images and modular curves, Proceedings of the Symposium on Algebraic Number Theory and Related Topics, 145–161, RIMS Kôkyûroku Bessatsu, **B32**, Res. Inst. Math. Sci. (RIMS), Kyoto, 2012.
- [3] *K. Arai, F. Momose*, Algebraic points on Shimura curves of $\Gamma_0(p)$ -type, to appear in J. Reine Angew. Math., available at the web page (<http://arxiv.org/pdf/1202.4841v2.pdf>).
- [4] *K. Buzzard*, Integral models of certain Shimura curves, Duke Math. J. **87** (1997), no. 3, 591–612.
- [5] *B. Jordan*, Points on Shimura curves rational over number fields, J. Reine Angew. Math. **371** (1986), 92–114.

- [6] *A. Kurihara*, On some examples of equations defining Shimura curves and the Mumford uniformization, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **25** (1979), no. 3, 277–300.
- [7] *B. Mazur*, Rational isogenies of prime degree (with an appendix by D. Goldfeld), Invent. Math. **44** (1978), no. 2, 129–162.
- [8] *F. Momose*, Isogenies of prime degree over number fields, Compositio Math. **97** (1995), no. 3, 329–348.
- [9] *G. Shimura*, On the real points of an arithmetic quotient of a bounded symmetric domain, Math. Ann. **215** (1975), 135–164.
- [10] *A. Weil*, Basic number theory, Reprint of the second (1973) edition. Classics in Mathematics. Springer-Verlag, Berlin, 1995.

(Keisuke Arai) Department of Mathematics, School of Engineering, Tokyo Denki University, 5 Senju Asahi-cho, Adachi-ku, Tokyo 120-8551 Japan
E-mail address: `araik@mail.dendai.ac.jp`